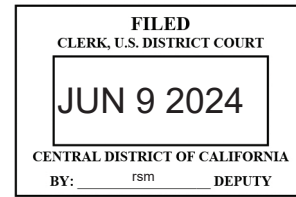


## UNITED STATES DISTRICT COURT

for the

Central District of California



UNITED STATES OF AMERICA

v.

WENHUI HUANG,

Defendant(s)

Case No. **2:24-MJ-03386**

**CRIMINAL COMPLAINT BY TELEPHONE  
OR OTHER RELIABLE ELECTRONIC MEANS**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Between on or about the date(s) of December 18, 2015 through March 12, 2024, in the counties of Los Angeles, Riverside, Orange, and San Bernardino, in the Central District of California, the defendant(s) violated:

*Code Section*

18 U.S.C. § 2320(a)(1)

*Offense Description*

Conspiracy to Traffic in Counterfeit Goods

This criminal complaint is based on these facts:

*Please see attached affidavit.*

☒ Continued on the attached sheet.

/s/ Jiongwei Cassidy Liu

*Complainant's signature*

Jiongwei Cassidy Liu, HSI Special Agent

*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: June 9, 2024

*Jean P. Rosenbluth*

*Judge's signature*

City and state: Los Angeles, California

Hon. Jean P. Rosenbluth, U.S. Magistrate Judge

*Printed name and title*

**AFFIDAVIT**

I, Jiongwei Cassidy Liu, being duly sworn, declare and state as follows:

**I. BACKGROUND OF AFFIANT**

1. I am a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations ("HSI"), and have been so employed since July 2022. From September 2022 to March 2023, I received training at the Federal Law Enforcement Training Center. This training included courses on conducting criminal investigations, narcotics identification, organized crime, gangs, fraud, counterfeiting, and other law enforcement topics. I have conducted multiple criminal investigations for violations of federal and state laws including, but not limited to fraud, narcotics, money laundering, trafficking, identity theft, and human trafficking and smuggling.

**II. PURPOSE OF AFFIDAVIT**

2. I make this affidavit in support of a complaint and arrest warrant for WENHUI HUANG ("HUANG") for a violation of 18 U.S.C. § 2320(a)(1) (Conspiracy to Traffic in Counterfeit Goods).

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and arrest warrant and does not purport to set forth all of my

knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, all amounts or sums are approximate, and all dates and times are on or about those indicated.

### **III. SUMMARY OF PROBABLE CAUSE**

4. On May 30, 2024, five defendants were arrested in the Central District of California on an indictment charging them in a multi-year, multi-million-dollar counterfeit Apple device scheme. In subsequent Mirandized interviews, two of those defendants (referred to hereinafter as co-conspirator 1 ("CC1") and co-conspirator 2 ("CC2")) identified HUANG as their source of counterfeit Apple devices. Both of those defendants were subsequently detained.

5. Further investigation into HUANG revealed that he had made hundreds of suspected fraudulent returns of counterfeit Apple devices, had received hundreds of shipments from China believed to contain counterfeit Apple devices, and had exchanged numerous text messages with other co-conspirators relating to the counterfeit Apple device conspiracy, among others.

6. On June 6, 2024, this Court issued a search warrant for HUANG's residence in Chino Hills, California 91709 (the "SUBJECT PREMISES"). Before the execution of that search warrant, HSI learned that HUANG and his girlfriend had booked one-way flights to China, with a scheduled departure of June 7, 2024, at 11:15 p.m., from Los Angeles International Airport, which HUANG had booked the day before.

7. At approximately 5:00 p.m. on Friday, June 7, 2024, agents and I spotted HUANG outside the SUBJECT PREMISES. HUANG was traveling in a car with a friend and his girlfriend at the time, and they were on their way to the airport with many pieces of luggage.

8. Based on the below facts demonstrating probable cause that HUANG was part of the counterfeit Apple device conspiracy, and the exigent circumstances of HUANG's imminent departure from the United States via a one-way flight to China, HSI arrested HUANG at approximately 5:25 p.m. on Friday, June 7, 2024.

#### **IV. STATEMENT OF PROBABLE CAUSE**

##### **A. Five Chinese Nationals Are Indicted for a Counterfeit Apple Device Scheme**

9. On May 23, 2024, five defendants were charged in a 22-count indictment with violations of 18 U.S.C. § 1349 (Conspiracy to Commit Wire and Mail Fraud); 18 U.S.C. § 1028A (Aggravated Identity Theft); 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 1341 (Mail Fraud); and 18 U.S.C. § 2320 (Conspiracy to Traffic in Counterfeit Goods). See United States v. Yang Song, et al., Case No. 2:24-CR-331-AB (C.D. Cal.). The charges stem from defendants' conspiracy to defraud Apple through the fraudulent return and attempted return of over 16,000 counterfeit Apple devices at Apple stores throughout the Central District of California between December 18, 2015 and at least March 12, 2024, thereby defrauding Apple of over \$12 million, as alleged in the indictment. Further background on the scheme can be

found in the indictment attached to this affidavit. See Ex. 1 at 31-61.<sup>1</sup>

10. On May 30, 2024, HSI arrested the five defendants, and executed federal search warrants.

11. The arrests were later publicized in a press release issued by the U.S. Attorney's Office on May 31, 2024, available at <https://www.justice.gov/usao-cdca/pr/chinese-nationals-arrested-alleged-123-million-fraud-involving-fraudulent-return>. These arrests were also publicized by various local media outlets, including KTLA 5, the Los Angeles Daily News, and other publications.

**B. Co-Conspirators Identified HUANG as Their Source of Counterfeit Apple Devices**

12. On May 30, 2024, HSI agents interviewed certain co-conspirators. Both were Mirandized and agreed to speak with law enforcement. The interviews were recorded and conducted in the Mandarin Chinese language. I speak Mandarin and personally interviewed CC2 and another Mandarin-speaking law enforcement agent interviewed CC1. The information provided below is based on a review of the recording of CC2's interview as well as a report prepared by the agent who interviewed CC1.

Interview of Co-Conspirator 1 ("CC1")

---

<sup>1</sup> Exhibit 1 is the partially redacted application in support of a search warrant for HUANG's residence (the SUBJECT PREMISES), Case No. 2:24-MJ-03322, and includes a copy of the indictment as well as a summary of other investigative steps relating to HUANG. Exhibit 1 is incorporated herein by reference. For the Court's convenience, the government has paginated Exhibit 1 with red page numbers and all pin cites in this affidavit are to those page numbers in red.

13. During CC1's interview, CC1 stated the following, among other things:

a. CC1 knew the Apple devices that he returned to Apple stores were fake but he did not believe it was illegal because Apple accepted the products.

b. CC1 stated that he made his living by working for HUANG to return these counterfeit Apple products.

c. CC1 started returning counterfeit Apple products in approximately 2015. CC1 met HUANG many years ago, through a mutual friend, and he stated their relationship is at least seven years old. CC1 was unaware of HUANG's specific date of birth, but knew he was born in 1984. CC1 reported that HUANG's contact in CC1's phone was listed as "Brother Huang."

d. CC1 reported that HUANG paid him \$50 per Apple device if the return is successful, i.e., he receives a new Apple device, and \$20 per unsuccessful return, i.e., Apple rejected the device.

e. CC1 stated that after he successfully exchanged counterfeit Apple devices for genuine Apple devices, he would provide the new authentic device to HUANG. CC1 did not know what HUANG would do with the device afterward.

f. CC1 indicated that as of this year, 2024, he was returning counterfeit Apple AirPods. However, in the prior year, he exchanged iPhone, iPads, and Apple watches. With respect to the AirPods activity in the past year, CC1 reported that he would purchase real AirPods at Target or Walmart stores. He would then copy the serial numbers for the real AirPods and

give these serial numbers to HUANG, whom he reported would then send these serial numbers to China. CC1 reported that HUANG would then later give CC1 counterfeit AirPods to fraudulently return at Apple stores, while CC1 would return the real AirPods back to Target and Walmart.

g. CC1 stated he recruited CC2 to make counterfeit returns of Apple devices at Apple stores. CC1 stated he would receive the devices from HUANG and provide them to CC2. CC1 stated that he would pay CC2 \$40 for every return, and that he would make \$10 per device that CC2 returned.

h. CC1 also said that he recruited other co-conspirators to make returns of suspected counterfeit Apple products.

i. CC1 stated that he did not have a set schedule for meeting with HUANG, but they would meet regularly, sometimes every week, and he would pick up counterfeit devices from HUANG at these meetings.

j. CC1 stated that HUANG lived at the SUBJECT PREMISES. CC1 identified HUANG's wife as D.H. and stated that HUANG has two children.

#### Interview of Co-Conspirator 2 ("CC2")

14. During CC2's interview, CC2 stated the following, among other things:

a. CC2 admitted that he made fraudulent returns of counterfeit Apple products at Apple stores.

b. CC2 stated he began returning counterfeit Apple devices in 2015, after being introduced to the business by his

friend, whom he identified as CC1. According to CC2, CC1 told him that the Apple devices they were returning had some real and some fake parts. CC2 said that, at first, he did not believe that there were fraudulent parts inside the Apple devices, but he began to suspect the devices had counterfeit parts as he made more and more returns.

c. CC2 stated that CC1 would receive the counterfeit Apple devices from a person named "HUANG." CC2 said he had only met HUANG two or three times. CC2 estimated that HUANG was approximately 40 years old.

d. CC2 reported that he saw other individuals of Chinese descent making suspected returns of counterfeit Apple devices at Apple stores, like he was doing. He reported that he overheard these individuals mentioning that all their fake devices come from HUANG.

**C. A Federal Search Warrant Was Issued for the SUBJECT PREMISES**

15. On June 6, 2024, the Honorable Karen L. Stevenson issued a search warrant for HUANG's residence, the SUBJECT PREMISES. See Case No. 2:24-MJ-03322; see also Ex. 1 (Application in Support of Search Warrant for SUBJECT PREMISES).

16. HSI agents planned to execute the search warrant on the SUBJECT PREMISES on the morning of Friday, June 7, 2024, but they did not because there was concern that HUANG had left his home. Specifically on June 6, 2024, HSI agents conducted surveillance at the SUBJECT PREMISES in the early morning hours and did not see signs of people inside the SUBJECT PREMISES.



However, the day before, on June 5, 2024, HSI agents surveilled the SUBJECT PREMISES and observed HUANG arrive at the SUBJECT PREMISES in the afternoon driving a white Tesla with California license plate 9GLF803 ("SUBJECT VEHICLE 1"), registered to D.H. at the SUBJECT PREMISES, according to DMV records.<sup>2</sup> HUANG parked SUBJECT VEHICLE 1 in the driveway and was seen exiting the vehicle with a female, who is believed to be D.H., and two children, who are believed to be his daughters. Agents also observed another car sitting in the driveway, a grey Toyota Sienna with California license plate 7AUY455 ("SUBJECT VEHICLE 2"), registered to HUANG at SUBJECT PREMISES, according to DMV records.

**D. HSI Learned of HUANG's Planned Flight to China**

17. On the morning of Friday, June 7, 2024, HSI received an alert that HUANG booked a one-way trip to China, via Sichuan Airlines Flight No. 3U3838, for himself and D.H. departing Los Angeles International Airport at 11:15 p.m. on Friday, June 7, 2024. HSI Special Agent Daniel A. Rocha contacted U.S. Customs and Border Protection ("CBP") Agent Ryan Benavietes who confirmed that HUANG booked the one-way flights at 11 p.m. on June 6, 2024.<sup>3</sup> No reservations for HUANG's two children were made on this flight.

---

<sup>2</sup> Law enforcement initially believed that HUANG and D.H. were married, however, they later learned from speaking with HUANG that he and D.H. are not married, but rather long-term partners and that they share two minor children together.

<sup>3</sup> According to review of CBP travel records, HUANG's last travel to China was in 2009.

18. Given law enforcement's inability to find HUANG at the SUBJECT PREMISES, I applied for search warrants for HUANG's person and SUBJECT VEHICLES 1 and 2 on the afternoon of June 7, 2024. See Case Nos. 2:24-MJ-03363, -3364, and -3370. The Honorable Karen L. Stevenson issued the search warrants for HUANG's person and SUBJECT VEHICLES 1 and 2 at approximately 4:00 p.m. on Friday, June 7, 2024.

**E. Further Review of HUANG's Involvement in the Apple Scheme**

19. Following the identification of HUANG as the potential source of counterfeit devices, HSI investigated HUANG and the SUBJECT PREMISES further. That investigation is summarized in Exhibit 1, including at pages 10, 22, and 23. Relevant here, HUANG incorporated an electronics repair business in 2019 at another address in Chino Hills, California, and HUANG received over 500 packages from China or Hong Kong at the SUBJECT PREMISES and two other addresses associated with him in Chino Hills, California. A significant number of these packages had cargo descriptions noting that these packages contained "used iPhone," "used tablet," "used mobile phone," or "electronic book reader," among other items. Based on my training and experience, as well as information provided by Apple relating to similar schemes, I am aware that some people involved in the counterfeit Apple device scheme describe packages containing counterfeit Apple devices as "used devices" on customs manifest in order to likely not raise suspicion about the counterfeit products.

20. On the afternoon of June 7, 2024, Apple provided updated data relating to suspected fraudulent returns of counterfeit devices made by HUANG and his partner, D.H. This Apple data showed that HUANG was associated with a total of 532 suspected fraudulent returns or attempted fraudulent returns of counterfeit Apple devices between 2018 and approximately March 2024. In addition, the name "huang wenhui," HUANG's first and last name transposed, was associated with another 43 returns, while HUANG's partner was associated with 21 returns.

21. Also, on June 7, 2024, a Mandarin-speaking agent began a preliminary review of two phones seized from CC1 pursuant to a federal search warrant. During the review of those phones, agents found lengthy WeChat messages between CC1 and "Brother Huang," whom CC1 earlier identified as HUANG. Throughout these extensive chats, CC1 and HUANG discussed the counterfeit Apple device scheme. These messages are in Mandarin Chinese, and excerpts below reflect preliminary translations by the Mandarin-speaking agent. Below are some examples of the messages and photos exchanged between CC1 and HUANG:

a. On May 9, 2024, HUANG sent CC1 a shipping label and indicated it was a shipment of AirPods.

b. On May 8, 2024, CC1 told HUANG that he saw two people attempt to return suspected counterfeit AirPods at a Target store. CC1 said that they examined the AirPods for a while and did not accept the return. HUANG responded they were probably too fake.

c. On December 26, 2023, HUANG sent CC1 a Chinese-language newspaper article about three individuals who were arrested in New York for fraud relating to counterfeit Apple products. HUANG then sent text messages saying that they must have returned too many iPads and people noticed.

d. On December 21, 2023, HUANG sent CC1 an audio message that a new shipment has arrived and he should start returning them once they arrive.

e. On November 26, 2023, CC1 sent HUANG an Apple store receipt and said that the Apple store replaced this device on-site. HUANG responded with the OK emoji.

f. On November 27, 2023, HUANG texted CC1 indicating that because it was Christmas time, they should do fewer repairs. In a voice message, CC1 agreed that they should not go to the stores as often during the week of Christmas. Based on my knowledge of the investigation, I know that many co-conspirators involved in the counterfeit Apple scheme describe their returns of suspected counterfeit devices as "repairs," which is the same terminology that Apple uses to describe the process to fix or replace an Apple device. Accordingly, I believe this to be a reference to the timing or frequency of repairs at Apple stores during the holidays.

g. On November 9, 2023, CC1 sent a text message to HUANG asking if the watches can be made to not power on because it has been two days and they still have battery power. CC1 sent a photo for four suspected counterfeit Apple watches. The

photo is of the watch body only, with no straps or Apple packaging.

h. On November 1, 2023, HUANG asked CC1 the best stores to accept repairs of suspected counterfeit Apple phones because HUANG would like to make appointments at those stores.

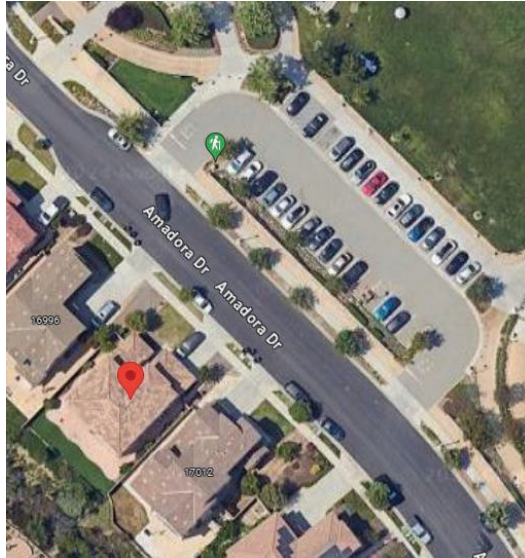
i. Throughout the text messages, HUANG and CC1 exchanged numerous spreadsheets tracking suspected counterfeit Apple devices which included information such as the Apple device, the serial number, the date of suspected return at Apple store, and the results of the return.

j. Throughout the text messages, HUANG and CC1 also exchanged numerous photos of suspected counterfeit Apple devices.

**F. HSI Agents Arrested HUANG and Executed Search Warrant at the SUBJECT PREMISES**

22. HSI agents continued to conduct surveillance on the SUBJECT PREMISES throughout the afternoon of Friday, June 7, 2024 to execute the search warrant on the SUBJECT PREMISES and HUANG's person. Agents did not immediately execute the search warrant due to the uncertainty of HUANG's location and his pending departure flight to China.

23. At approximately 5:00 p.m., I was on surveillance and parked in a parking lot directly across from the SUBJECT PREMISES. Below is a Google maps satellite photo showing the parking lot across from the SUBJECT PREMISES where I parked.



24. While in the parking lot, I observed an Asian male, who was later identified as HUANG's friend, exiting a car parked directly to the right of my surveillance car in the parking lot and walk towards the SUBJECT PREMISES. The Asian male opened the front door of the SUBJECT PREMISES and remained inside for less than five minutes before walking out to briefly examine the trash cans belonging to the SUBJECT PREMISES located next to the curb of the SUBJECT PREMISES. The Asian male was seen talking on a cellphone throughout this time. Meanwhile, I also observed another Asian male who bore a slight resemblance to HUANG sitting in the passenger side of the car parked to my right. I observed him looking around the parking lot and across the street while he was also talking on a cellphone, and I began to believe that he might possibly to talking to the first Asian male.

25. The first Asian male then walked back to the driver's side of his car in the parking lot and was about to drive away.

At that moment, other agents and I contacted this car and the occupants inside. Agents ordered all three occupants to exit the car. The male passenger identified himself as HUANG and an Asian female passenger in the backseat of the car identified herself as D.H.

26. HUANG asked me in Chinese Mandarin why he was being detained. I told him it was related to Apple fraud. HUANG then nodded and hesitated for a few seconds before asking me if it was related to the prior week's arrests related to the Apple fraud. I replied yes. He made no further comments to me at that time.

27. Agents arrested HUANG and temporarily detained D.H. and the first Asian male who identified himself as X.W. HUANG told me that he had a flight later that night to China and that he needed to find a way to cancel his flights because the tickets were very expensive.

28. Agents asked for verbal consent to search the friend's vehicle. The friend agreed. Inside the vehicle were several pieces of luggage and dozens of Apple devices which included approximately twenty-five boxes of AirPods, ten Apple Watch devices without watch bands (without boxes), and fifteen iPhones (without boxes).

29. I mirandized HUANG in Chinese Mandarin and HUANG asked to speak to an attorney.

30. Agents later spoke to D.H. She stated that they were traveling to China to take care of HUANG's ailing parents. D.H. also stated that their children were staying with friends.

31. As part of the search, agents asked HUANG where SUBJECT VEHICLES 1 and 2 were located in order to execute the search warrants on those vehicles. HUANG told agents that he sold both cars to CarMax.

32. While HUANG was placed under arrest, agents began executing the search warrant on the SUBJECT PREMISES. HUANG told agents that they would not find anything in the house nor on his cellphones.

33. Agents searched the house and found approximately twenty electronic devices, including laptops, tablets, and cellphones.

34. Agents also searched the trash cans that were left on the street in front of the SUBJECT PREMISES. Inside were plastic bags full of Apple receipts and other documents relating to Apple returns and purchases.

35. HUANG was transported to and later booked at Hawthorne Police Department jail that evening.

36. Accordingly, for the foregoing reasons, there is probable cause that HUANG was conspiring with others, including CC1 and CC2, as part of a conspiracy involving counterfeit Apple goods, in addition to probable cause that HUANG was attempting to flee the United States in light of his co-conspirators' arrests. The conduct described above is consistent with HUANG participating in the Apple return fraud scheme charged in United States v. Yang, et al., Case No. 2:24-CR-331-AB (C.D. Cal.).



**V. CONCLUSION**

37. For all the reasons described above, there is probable cause to believe that HUANG violated 18 U.S.C. § 2320(a)(1) (Conspiracy to Traffic in Counterfeit Goods).

/s/ Cassidy Liu  
Jiongwei Cassidy Liu, Special  
Agent  
Homeland Security Investigations

Attested to by the applicant in  
accordance with the requirements  
of Fed. R. Crim. P. 4.1 by  
telephone on this 9th day of June,  
2024.



THE HONORABLE JEAN P. ROSENBLUTH  
UNITED STATES MAGISTRATE JUDGE

# Exhibit 1

## UNITED STATES DISTRICT COURT

for the  
Central District of California

In the Matter of the Search of )  
The premises located at [REDACTED], )  
Chino Hills, California 91709 ("SUBJECT ) Case No. 2:24-MJ-03322  
PREMISES"), as further described in Attachment A )  
)  
)

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

*See Attachment A*

located in the Central District of California, there is now concealed (*identify the person or describe the property to be seized*):

*See Attachment B*

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1349	Conspiracy to Commit Wire and Mail Fraud
18 U.S.C. § 1028A	Aggravated Identity Theft
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1341	Mail Fraud
18 U.S.C. § 2320	Conspiracy to Traffic in Counterfeit Goods

The application is based on these facts:

*See attached Affidavit*

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (*give exact ending date if more than 30 days: \_\_\_\_\_*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*/s/ Jiongwei Cassidy Liu*

*Applicant's signature*

Jiongwei Cassidy Liu, HSI Special Agent

*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: June 6, 2024

City and state: Los Angeles, CA

AUSA: Andrew Roach (x0306)

*Karen L. Stevenson*

*Judge's signature*

Honorable Karen L. Stevenson, U.S. Magistrate Judge

*Printed name and title*

**ATTACHMENT A**

**PROPERTY TO BE SEARCHED**

The premises to be searched is the property located at [REDACTED], Chino Hills, California 91709 ("SUBJECT PREMISES").

**EXTERIOR OF THE SUBJECT PREMISES**



**ATTACHMENT B**

**I. ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1349 (Conspiracy to Commit Wire and Mail Fraud); 18 U.S.C. § 1028A (Aggravated Identity Theft); 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 1341 (Mail Fraud); and 18 U.S.C. § 2320 (Conspiracy to Traffic in Counterfeit Goods) (the "Subject Offenses"), namely:

a. All communications, records, and other evidence reflecting or relating to the Subject Offenses;<sup>4</sup>

b. All communications, records, and other evidence relating to or reflecting the identity or location of co-conspirators engaged in the Subject Offenses;

c. All communications, records, and other evidence reflecting or relating to the identification of persons, businesses, or entities that manufacture or sell counterfeit Apple or other electronic devices;

d. All communications, records, and other evidence reflecting or relating to methods used to obtain Apple serial numbers and/or IMEI numbers under warranty with Apple;

e. All communications, records, and other evidence of suspected counterfeit Apple or other electronic devices;

---

<sup>4</sup> As used here, "evidence" refers to evidence all forms, whether it be electronic, physical, tangible, or intangible.

f. All communications, records, and other evidence relating to the fraudulent return or exchange of suspected counterfeit Apple devices;

g. All communications, records, and other evidence relating to any person's visits to any Apple store;

h. All communications, records, and other evidence reflecting or relating to the identification of unlawfully obtained Apple device serial numbers and IMEI numbers;

i. All communications, records, and other evidence relating to the alteration of Apple device serial numbers and/or IMEI numbers;

j. All communications, records, and other evidence relating to the identification of persons, businesses, or entities that are involved in the distribution of stolen Apple serial numbers and/or IMEI numbers under Apple warranty;

k. All communications, records, and other evidence reflecting or relating to the sale, shipment, or smuggling of counterfeit iPhone, iPads, or other Apple devices, including but not limited to information about techniques used to ship counterfeit iPhones, iPads, or other Apple devices into the United States, and any documentation or records relating to the importation of counterfeit iPhones, iPads, or other Apple devices into the United States;

l. All communications, records, and other evidence relating to shipment of any genuine or counterfeit Apple products;

m. All communications, records, and other evidence relating to any mailbox or shipping method used as part of the Subject Offenses;

n. All communications, records, and other evidence reflecting or relating to the exportation of genuine iPhones, iPads, or other Apple devices from the United States;

o. All communications, records, and other evidence reflecting or relating to the identification of persons that receive counterfeit iPhones, iPads, or other Apple devices, and who exchange counterfeit iPhones, iPads, or other Apple devices for genuine ones;

p. All communications, records, and other evidence regarding the scheduling of appointments with Apple, including communications between co-conspirators regarding such appointments;

q. All communications, records, and other evidence reflecting or relating to identification of post office addresses, mailboxes, or other locations used to receive counterfeit Apple devices and replacement Apple devices;

r. All communications, records, and other evidence relating to payment, banking, or other financial information related to the receipt, exchange, or sale of iPhones, iPads, or other Apple devices;

s. All communications, records, and other evidence relating to or reflecting any person's motive or state of mind in relation to the Subject Offenses; and

t. All suspected proceeds of the Subject Offenses in whatever form they maybe, including cash, high-value items, cryptocurrency, etc.

2. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

3. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;



g. records of or information about Internet Protocol addresses used by the device.

4. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

## **II. SEARCH PROCEDURE FOR DIGITAL DEVICES**

6. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK"

(Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the scope of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the scope of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the scope of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been

able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

7. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

8. During the execution of this search warrant, with respect to any person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that falls within the scope of the warrant, law enforcement personnel are authorized to: (1) depress the thumb- and/or fingerprints of the person onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of the person with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of

any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

9. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

**AFFIDAVIT**

I, Jiongwei Cassidy Liu, being duly sworn, declare and state as follows:

**I. BACKGROUND OF AFFIANT**

1. I am a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations ("HSI"), and have been so employed since July 2022. From September 2022 to March 2023, I received training at the Federal Law Enforcement Training Center. This training included courses on conducting criminal investigations, narcotics identification, organized crime, gangs, fraud, counterfeiting, and other law enforcement topics. I have conducted multiple criminal investigations for violations of federal and state laws including, but not limited to fraud, narcotics, money laundering, trafficking, identity theft, and human trafficking and smuggling.

**II. PURPOSE OF AFFIDAVIT**

2. I make this affidavit in support of an application for warrant to search the residence of Wenhui Huang, located at [REDACTED], Chino Hills, California 91709 (the "SUBJECT PREMISES"), as further described in Attachment A.

**III. PLACE TO BE SEARCHED**

3. The place to be searched is SUBJECT PREMISES, as described in Attachment A.

**IV. ITEMS TO BE SEIZED**

4. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of

18 U.S.C. § 1349 (Conspiracy to Commit Wire and Mail Fraud); 18 U.S.C. § 1028A (Aggravated Identity Theft); 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 1341 (Mail Fraud); and 18 U.S.C. § 2320 (Conspiracy to Traffic in Counterfeit Goods) (the "Target Counterfeit Good Offenses"), as more fully described in Attachment B. Attachments A and B are incorporated herein by reference.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, all amounts or sums are approximate, and all dates and times are on or about those indicated.

#### **V. SUMMARY OF PROBABLE CAUSE**

6. On May 23, 2024, defendants YANG SONG ("SONG"), JUNWEI JIANG ("JIANG"), ZHENGXUAN HU ("HU"), YUSHAN LIN ("LIN"), and SHUYI XING ("XING") were charged in a 22-count indictment with violations of 18 U.S.C. § 1349 (Conspiracy to Commit Wire and Mail Fraud); 18 U.S.C. § 1028A (Aggravated Identity Theft); 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 1341 (Mail Fraud); and 18 U.S.C. § 2320 (Conspiracy to Traffic in Counterfeit Goods). See United States v. Yang Song, et al., Case No. 2:24-

CR-00331-AB (C.D. Cal.). The charges stem from defendants' conspiracy to defraud Apple through the fraudulent return and attempted return of over 16,000 counterfeit Apple devices between December 18, 2015 and through at least March 12, 2024, as alleged in the indictment. The case has been assigned to the Honorable André Birotte Jr., United States District Judge of the Central District of California.<sup>1</sup>

7. On May 30, 2024, HSI agents arrested the five above-named defendants [REDACTED]  
[REDACTED] [REDACTED]. In later, Mirandized interviews, [REDACTED] [REDACTED] and [REDACTED] stated they received their counterfeit Apple devices from Wenhui Huang ("HUANG"). [REDACTED] indicated that HUANG lives at SUBJECT PREMISES. Further review of evidence collected during the investigation revealed that HUANG received numerous shipments from China of suspected counterfeit devices at the SUBJECT PREMISES over the years of the scheme, in addition to the SUBJECT PREMISES being used as the shipping address for over 200 suspected fraudulent returns of counterfeit Apple devices to Apple, based on Apple data.

---

<sup>1</sup> On May 28, 2024, the assigned AUSA emailed Judge Birotte's Courtroom Deputy Clerk to inform the Court of the initial search warrant applications [REDACTED]  
[REDACTED]. The Courtroom Deputy Clerk informed the government that such warrants should be filed with the Duty Magistrate Judge. Accordingly, the government is filing this application for the search warrant before the Duty Magistrate Judge.



8. Accordingly, there is probable cause that evidence, fruits, and instrumentalities of violations of Target Counterfeit Good Offenses will be found at the SUBJECT PREMISES.

**VI. STATEMENT OF PROBABLE CAUSE**

**A. Defendants Are Indicted for the Target Counterfeit Good Offenses**

9. On May 23, 2024, in the Central District of California, defendants SONG, JIANG, HU, LIN, and XING were indicted on the Target Counterfeit Good Offenses. See United States v. Yang Song, et al., Case No. 2:24-CR-00331-AB (C.D. Cal.). The indictment is attached as **Exhibit 1** and is incorporated herein by reference.

10. The indictment alleges that between December 18, 2015 through at least March 12, 2024, defendants conspired with each other to fraudulently return and attempt to return counterfeit Apple devices to Apple stores throughout the Central District of California, thereby defrauding Apple of over \$12 million. Further background on the scheme is provided below.

**B. Background on Apple Warranty Fraud Scheme Involving Counterfeit Apple Products**

11. Based on my review of information provided by Apple, I am aware of the following information regarding Apple's warranty program and the scheme in which defendants SONG, JIANG, HU, LIN, and XING were involved:

a. Apple provides a one-year warranty for new iPhones and iPads that warrants against product defects and allows consumers to return a non-functioning device to Apple or

an Apple-authorized reseller and receive a replacement in exchange. Apple also sells iPhone and iPad insurance protection plans that extend beyond one year and similarly allow a customer to return a non-functioning iPhone or iPad and receive a replacement iPhone or iPad in exchange.

b. Criminals are aware of Apple's return policies and seek to exploit them by passing off counterfeit devices altered to look like non-functioning but in-warranty iPhones or iPads and exchanging them for replacement iPhones and iPads. Apple has investigated several cases of criminal organizations attempting to return these counterfeit Apple products to Apple in exchange for replacement iPhones and iPads.

c. According to Apple's investigations, one very common scheme works as follows: criminal organizations in China and Hong Kong fraudulently obtain serial numbers/IMEI numbers of in-warranty iPhones/iPads and apply these fraudulent serial numbers/IMEI numbers to non-operative devices that appear to be iPhones or iPads, but which are in fact assembled by co-conspirators with damaged or inoperative parts in order to pass them off as genuine, in-warranty Apple products.<sup>2</sup> Many such

---

<sup>2</sup> All genuine Apple iPhones and iPads have unique electronic IMEI serial numbers. The IMEI number is an industry standard system used to identify a device and to help prevent theft. The electronic serial numbers are integral to Apple's comprehensive quality control and inventory tracking processes, and they enable Apple to track a variety of information about a particular unit, such as the time and place of production, and whether the unit was approved for sale. Removing and/or altering serial numbers or IMEI numbers of Apple iPhones or iPads interferes with Apple's ability to control the quality of its products bearing the Apple trademarks and the experience of

*(footnote cont'd on next page)*

products contain parts that bear spurious Apple trademarks and/or that were not made or approved by Apple or its licensees.

d. The criminals then ship these counterfeit iPhones and iPads to countries all over the world, including the United States and, specifically here, the Central District of California, where they work with in-country co-conspirators, such as the defendants in this case, to pass them off as authentic, in-warranty iPhones and iPads to Apple or Apple's authorized service providers so that they can be exchanged for authentic iPhones and iPads.

e. The fraudulently obtained genuine Apple products are then often aggregated and shipped back to Hong Kong and smuggled into China to avoid the VAT tax, where they are then sold to consumers, and are often boxed with counterfeit Apple product accessories and packaging.

f. As part of an investigation in the Los Angeles, California area, Apple determined that SONG, JIANG, HU, LIN, and XING were associated with over approximately 16,000 fraudulent returns and attempted returns of suspected counterfeit devices during the course of the scheme. Apple also examined multiple devices returned by defendants SONG, JIANG, HU, LIN, and XING over the course of the scheme. Apple's examination of these devices showed that they were counterfeit Apple devices that had been returned to Apple stores under Apple's warranty programs.

---

Apple customers whose serial numbers/IMEI numbers are improperly replicated. As a result, an iPhone or iPad without an accurate serial number/IMEI number is not an authentic iPhone or iPad.

**C. HSI Arrests Defendants** [REDACTED]  
[REDACTED]

12. On May 30, 2024, HSI arrested the five charged defendants [REDACTED] [REDACTED]  
[REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

13. [REDACTED] [REDACTED]  
[REDACTED], agents seized approximately \$160,000 in cash and approximately 150 suspected counterfeit Apple AirPods.

**D. [REDACTED] Identified HUANG as Their Source of Counterfeit Apple Devices**

14. That same day, May 30, 2024, HSI agents interviewed [REDACTED]. Both were Mirandized and agreed to speak with law enforcement. The interviews were recorded and conducted in the Mandarin language. I speak Mandarin and personally interviewed [REDACTED] and another Mandarin-speaking law enforcement agent interviewed [REDACTED]. The information provided below is based on review of the recording of [REDACTED] interview as well as a report prepared from the agent who interviewed [REDACTED]

Interview of [REDACTED] [REDACTED]

15. During [REDACTED] interview, [REDACTED] stated the following, among other items:

a. [REDACTED] knew the Apple devices that he returned to Apple stores were fake but he did not believe it was illegal because Apple accepted the products.

b. [REDACTED] stated that he made his living by working for HUANG to return these counterfeit Apple products.

c. [REDACTED] started returning counterfeit Apple products in approximately 2015. [REDACTED] met HUANG many years ago, through a mutual friend, and he stated their relationship is at least seven years old. [REDACTED] was unaware of HUANG's specific date of birth, but knew he was born in 1984.

d. [REDACTED] reported that HUANG paid him \$50 per Apple device if the return is successful, i.e., he receives a new Apple device, and \$20 per unsuccessful return, i.e., Apple rejected the device.

e. [REDACTED] stated that after he successfully exchanged counterfeit Apple devices for genuine Apple devices, he would provide the new authentic device to HUANG. [REDACTED] did not know what HUANG would do with the device afterward.

f. [REDACTED] indicated that as of this year, 2024, he was now working with counterfeit Apple AirPods. However, in the prior year, he was exchanging iPhone, iPads, and Apple watches. With respect to the AirPods activity within the past year, [REDACTED] reported that he would purchase real AirPods at Target or Walmart stores. He would then copy the serial numbers for the

real AirPods and give these serial numbers to HUANG, whom he reported would then send these serial numbers to China. [REDACTED] reported that HUANG would then later give [REDACTED] counterfeit AirPods to fraudulently return at Apple stores, while [REDACTED] would return the real AirPods back to Target and Walmart.

g. [REDACTED] stated he recruited [REDACTED] to make counterfeit returns of Apple devices at Apple stores. [REDACTED] stated he would receive the devices from HUANG and provide them to [REDACTED]. [REDACTED] stated that he would pay [REDACTED] \$40 for every return, and that he would make \$10 per device that [REDACTED] returned.

h. [REDACTED] also said that he recruited [REDACTED] and [REDACTED] to make returns of suspected counterfeit Apple products.

i. [REDACTED] stated that he does not have a set schedule of meeting HUANG, but they would meet regularly, sometimes every week, sometimes longer, where he would pick up counterfeit devices.

j. [REDACTED] stated that HUANG lived at the SUBJECT PREMISES. [REDACTED] identified HUANG's wife as D [REDACTED] H [REDACTED] and stated that HUANG has two children.

Interview of [REDACTED] [REDACTED]

16. During [REDACTED] interview, [REDACTED] stated the following, among other items:

a. [REDACTED] admitted that he made fraudulent returns of counterfeit Apple products at Apple stores.

b. [REDACTED] stated he began returning counterfeit Apple devices in 2015, after being introduced to the business by his

friend, whom he identified as [REDACTED]. According to [REDACTED], [REDACTED] told him that the Apple devices they were returning had some real and some fake parts. [REDACTED] said that, at first, he did not believe that there were fraudulent parts inside the Apple devices, but he began to suspect the devices had counterfeit parts as he made more and more returns.

c. [REDACTED] stated that [REDACTED] would receive the counterfeit Apple devices from a person named "HUANG." [REDACTED] said he had only met "HUANG" two or three times. [REDACTED] [REDACTED] estimated that he was approximately 40 years old.

d. [REDACTED] [REDACTED] reported that he saw other individuals of Chinese descent making suspected returns of counterfeit Apple devices at Apple stores, like he was doing. He reported that he overheard these individuals mentioning about how all their fake devices come from "HUANG."

**E. Apple Data Shows SUBJECT PREMISES Was Used For Hundreds of Suspected Fraudulent Returns of Apple Devices**

17. Apple produced information relating to the suspected fraudulent returns of counterfeit Apple devices to HSI as part of the investigation.

18. According to this Apple data, the SUBJECT PREMISES was listed as the shipping address to receive new genuine Apple products for which suspected counterfeit devices had been returned in over 200 instances between approximately 2021 and 2023, with one return associated with the SUBJECT PREMISES in June 2023. The vast majority of these returns were in [REDACTED] name.

19. Apple data also revealed that approximately 28 suspected fraudulent returns of Apple devices were by an individual named "Wenhui huang" in 2017. However, Apple had limited data on these returns given their age.

**F. Further Investigation in HUANG**

20. According to California DMV records, HUANG's date of birth is [REDACTED] 1984, and he resides at the SUBJECT PREMISES.

21. According to the California Secretary of State reports, HUANG incorporated a corporation called "Chuang Long Company" on July 8, 2019. This filing listed the business address as [REDACTED], Chino Hills, CA 91709, which according to law enforcement databases is an address associated with HUANG. Later corporate filings for this company listed its business type as "electronic parts repair."

22. I attempted to search for information about Chuang Long Company online to see if it had a website or any public storefront. I was unable to find any website or storefront associated with the business.

23. HSI received Customs and Border Protection ("CBP") international shipment records for the SUBJECT PREMISES. Those records showed that between 2021 and 2024, HUANG received approximately 80 packages from Hong Kong or China at the SUBJECT PREMISES. Most of the cargo descriptions of these packages, approximately 77 packages, noted that these packages included some "used" electronics, such as "used iPhone," "used tablet," "used mobile phone," or "electronic book reader."



24. In addition, CBP records showed similar shipments of used electronics being shipped to HUANG at two other addresses associated with him in Chino Hills, California: (1) [REDACTED] and (2) [REDACTED].

25. CBP records showed approximately 398 shipments from China to HUANG at [REDACTED], Chino Hills, California, between February 3, 2019 and January 23, 2023. Of those, approximately 150 packages had cargo descriptions noting some form of used electronics, including "used iPhone," "used tablet," "used mobile phone," or "electronic book reader."

26. CBP records also showed approximately 112 shipments from China to HUANG at [REDACTED], Chino Hills, California, between January 29, 2021 and January 26, 2022. Approximately 70 of these packages had cargo descriptions suggesting some electronic devices, including "tablet PC" and "used tablet"

27. Based on my training and experience as well as information that I learned from Apple from other investigations involving counterfeit Apple devices, I know that people who engage in the trade of counterfeit electronic will sometimes create electronic repair companies to import counterfeit devices from China. It is believed that this is done through the company in order to not arouse suspicions regarding the importation of devices from China.

**G. Recent Surveillance of the SUBJECT PREMISES Shows HUANG**

28. HSI conducted surveillance of the SUBJECT PREMISES on June 5, 2024. During the surveillance, agents observed HUANG

arrive at SUBJECT PREMISES in a white Tesla with California license plate 9GLF803, which is registered to HUANG's wife at SUBJECT PREMISES, according to DMV records. HUANG was observed exiting the vehicle with a female, who is believed to be his wife, and two children, who are believed to be his daughters. Agents also observed another car sitting in the driveway, a grey Toyota Sienna with California license plate 7AUY455, which is registered to HUANG at SUBJECT PREMISES, according to DMV records.

**H. There is Probable Cause that Evidence of the Target Counterfeit Device Offenses Will Be Found at the SUBJECT PREMISES**

29. Based on my training and experience and knowledge of the investigation, I know the counterfeit device scheme against Apple has generated significant electronic evidence, including electronic evidence that is suspected of being on individuals' digital devices at their SUBJECT PREMISES. For example, Apple sent multiple emails and text messages associated with each and every return of an Apple device. Law enforcement has seen examples of such emails in [REDACTED] [REDACTED] [REDACTED] and [REDACTED] email accounts from prior search warrants and more is expected to be found on the digital devices of those involved in the scheme. In addition, digital devices of those involved in the scheme are likely to contain those individuals' WeChat

communications related to the fraud, a portion of which investigators have seen through other search warrants.

30. Further, there is probable cause that physical evidence of the Target Counterfeit Device Offenses will be found at the SUBJECT PREMISES. As mentioned above, [REDACTED] and others have been engaged in the Target Counterfeit Device Offenses recently, including within the past six months relating to counterfeit AirPods (which he received from HUANG), and there is probable cause that evidence of the counterfeit devices, including counterfeit devices themselves, shipping information, and other related evidence, will be found at the SUBJECT PREMISES.

#### **VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES<sup>3</sup>**

31. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained

---

<sup>3</sup> As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

32. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

33. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person

may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, if while executing the warrant, law enforcement personnel encounter a digital device within the scope of the warrant that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to every person who is located at the SUBJECT PREMISES during the execution of the search who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that falls within the scope of the warrant:

(1) depress the person's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

//

//

//

**VIII. CONCLUSION**

34. For all the reasons described above, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of Target Counterfeit Good Offenses will be found at the SUBJECT PREMISES, as described in Attachment A.

/s/ Cassidy Liu  
Jiongwei Cassidy Liu, Special  
Agent  
Homeland Security Investigation

Attested to by the applicant in  
accordance with the requirements  
of Fed. R. Crim. P. 4.1 by  
telephone on this 6th day of June,  
2024.

Karen L. Stevenson  
THE HONORABLE KAREN L. STEVENSON  
UNITED STATES MAGISTRATE JUDGE



# Exhibit 1



UNITED STATES DISTRICT COURT  
FOR THE CENTRAL DISTRICT OF CALIFORNIA  
October 2023 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

YANG SONG,  
JUNWEI JIANG,  
ZHENGXUAN HU,  
YUSHAN LIN, and  
SHUYI XING,

Defendants.

CR No. 2:24-cr-00331-AB

I N D I C T M E N T

[18 U.S.C. § 1349: Conspiracy to Commit Wire Fraud and Mail Fraud; 18 U.S.C. § 1028A: Aggravated Identity Theft; 18 U.S.C. § 1343: Wire Fraud; 18 U.S.C. § 1341: Mail Fraud; 18 U.S.C. § 2320: Conspiracy to Traffic in Counterfeit Goods; 18 U.S.C. § 2(a): Aiding and Abetting; 18 U.S.C. §§ 981(a)(1)(C), 2323(b), and 28 U.S.C. § 2461(c): Criminal Forfeiture]

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS AND DEFINITIONS

At all times relevant to this Indictment:

Trademarks and Counterfeit Marks

1. A "trademark" is a word, phrase (such as a logo), symbol or design (such as an icon), or a combination thereof, which identifies and distinguishes the source of the goods of one particular manufacturer from those of other manufacturers. A trademark is often

1 a valuable asset, equated with the goodwill of a business  
2 organization, which can influence consumers in purchasing decisions.  
3 A "design mark" and a "standard character mark" are types of  
4 trademarks. Trademarks are registered for use in connection with  
5 particular types of goods or services.

6 2. A trademark serves a variety of purposes. First, it avoids  
7 product confusion by allowing consumers to have confidence that two  
8 products for sale bearing the identical trademark were manufactured  
9 by the same company and will be of the same quality. Second, it  
10 permits consumers to make an informed choice to purchase a name-brand  
11 good based upon past experience, word-of-mouth, brand loyalty, and  
12 advertising impact. Third, it enables consumers who experience a  
13 problem with the name-brand product they have purchased to seek  
14 recourse through the actual manufacturer by returning the goods to  
15 the seller or seeking warranty or other recourse through the  
16 manufacturer. Fourth, it allows the trademark owner to distinguish  
17 and protect its products by giving that company exclusive rights as  
18 the trademark owner. This permits the legitimate trademark owner to  
19 recoup investments of time, money, labor, and creativity and to  
20 profit from its endeavors in bringing a particular product to market.

21 3. A counterfeit mark is: (a) a spurious mark used in  
22 connection with trafficking in goods; (b) identical with, or  
23 substantially indistinguishable from, a mark registered for those  
24 goods or services on the principal register of the United States  
25 Patent and Trademark Office and in use, whether or not defendants  
26 knew such mark was so registered; (c) that is applied to or used in  
27 connection with the goods or services for which the mark is  
28

1 registered; and (d) the use of which was likely to cause confusion,  
2 to cause mistake, or to deceive.

3 Apple Inc.

4 4. Apple Inc. ("Apple") was a multinational corporation that  
5 designed, developed, and sold consumer electronic devices, including  
6 the Apple iPhone ("iPhone"), the Apple iPad ("iPad"), and other  
7 devices, such as the Apple Watch, Apple Pencil, and AirPods. The  
8 United States Patent and Trademark Office had registered on its  
9 principal register a number of trademarks for Apple for use in  
10 connection with computer hardware and software of a wide variety,  
11 including handheld and mobile computers and peripherals, including  
12 the following, all of which were in use at all times relevant to this  
13 Indictment:

14 a. Trademark number 3,679,056, which registered the Apple  
15 logo design mark, as shown below;



20 b. Trademark number 3,928,818, which registered the Apple  
21 standard character mark, as shown below;

22 **APPLE**

23  
24 c. Trademark number 3,669,402, which registered the Apple  
25 iPhone standard character mark, as shown below; and

26 **iPhone**  
27  
28

1 d. Trademark number 4,537,934, which registered the Apple  
2 iPad standard character mark, as shown below.

3  
4 **IPAD**

5 5. All genuine Apple iPhones had an International Mobile  
6 Equipment Identity ("IMEI") number and serial number that were unique  
7 to each device. All genuine Apple iPads had a serial number that was  
8 unique to each device, and iPads with cellular connectivity also had  
9 an IMEI number that was unique to each device. All other genuine  
10 Apple devices had serial numbers unique to the device. Removing or  
11 altering IMEI or serial numbers of Apple devices interfered with  
12 Apple's ability to control the quality of its products bearing the  
13 Apple marks, and the experience of Apple customers whose IMEI and  
14 serial numbers were improperly replicated. As a result, Apple  
15 iPhones, iPads, and other devices without an accurate IMEI or serial  
16 number were not authentic Apple devices.

17 6. Apple provided a one-year warranty for new iPhones, iPads,  
18 and other devices that warranted against product defects and allowed  
19 customers to return a non-functioning device to Apple or an  
20 authorized Apple reseller and receive a replacement device. Apple  
21 also sold insurance protection plans, such as AppleCare+, that  
22 extended beyond one year and covered accidental damage and similarly  
23 allowed a customer to return a non-functioning Apple device and  
24 receive a replacement in exchange. It was the general practice of  
25 Apple to exchange broken iPhones, iPads, and other devices that were  
26 covered by an Apple warranty for new genuine iPhone, iPad, or device  
27 for a nominal fee.

1           7. A counterfeit Apple device was a device not assembled or  
2 manufactured by Apple but appearing to be an iPhone, iPad, or other  
3 Apple device, and bearing one or more counterfeit marks, to wit,  
4 marks identical with or substantially indistinguishable from one or  
5 more of the above-described trademarks registered by Apple. The  
6 counterfeit marks were each likely to cause confusion, to cause  
7 mistake, or to deceive.

1 COUNT ONE

2 [18 U.S.C. § 1349]

3 [ALL DEFENDANTS]

4 The Grand Jury hereby realleges and incorporates by reference  
5 paragraphs 1 through 7 of the Introductory Allegations and  
6 Definitions of this Indictment as though fully set forth herein.

7 A. OBJECTS OF THE CONSPIRACY

8 1. Beginning on an unknown date but no later than December 18,  
9 2015, and continuing through at least March 12, 2024, in Los Angeles,  
10 San Bernardino, Riverside, and Orange Counties, within the Central  
11 District of California, and elsewhere, defendants YANG SONG ("SONG"),  
12 JUNWEI JIANG ("JIANG"), ZHENGXUAN HU ("HU"), YUSHAN LIN ("LIN"), and  
13 SHUYI XING ("XING") knowingly and willfully conspired and agreed with  
14 each other, and other persons known and unknown to the Grand Jury, to  
15 commit wire fraud, in violation of Title 18, United States Code,  
16 Section 1343, and mail fraud, in violation of Title 18, United States  
17 Code, Section 1341.

18 B. MANNER AND MEANS OF CONSPIRACY

19 2. The objects of the conspiracy were carried out, and to be  
20 carried out, in substance, as follows:

21 a. Defendants SONG and JIANG, and other co-conspirators  
22 located in the United States, coordinated with co-conspirators in  
23 China to ship counterfeit Apple iPhones, iPads, and other devices to  
24 defendants SONG and JIANG, and other co-conspirators in the United  
25 States. The counterfeit Apple devices shipped to the United States  
26 were designed to look like genuine Apple devices and included  
27 identification numbers (IMEI and serial numbers) matching genuine  
28 identification numbers on real Apple devices that had been sold in

1 the United States and Canada, were owned by real persons, and under  
2 warranty through Apple's manufacturer warranty or AppleCare+.

3 b. Defendants SONG, JIANG, HU, LIN, and XING, and other  
4 co-conspirators, rented or caused to be rented mailboxes at numerous  
5 U.S. Post Offices, United Parcel Service ("UPS") Stores, and other  
6 commercial mailbox rental businesses for the purpose of the scheme.

7 c. Co-conspirators in China mailed the counterfeit Apple  
8 devices to multiple addresses throughout the Central District of  
9 California.

10 d. Defendants SONG, JIANG, HU, LIN, and XING, and other  
11 co-conspirators, then fraudulently returned the counterfeit Apple  
12 iPhones, iPads, and other devices to Apple as if the counterfeit  
13 Apple devices they returned were genuine Apple devices that had been  
14 legitimately purchased and were eligible for Apple's warranty  
15 programs and that defendants were the lawful possessors of the real  
16 Apple devices bearing the IMEI and serial numbers that were on the  
17 counterfeit Apple devices. Defendants and their co-conspirators  
18 fraudulently represented that the counterfeit Apple devices they  
19 returned were genuine Apple devices that were broken or non-  
20 operational and therefore were covered by Apple's warranty programs.  
21 Defendants and their co-conspirators, however, knew that the devices  
22 they returned were actually counterfeit Apple devices and not covered  
23 by Apple's warranty programs and that the real Apple devices bearing  
24 the IMEI and serial numbers listed on the counterfeit devices were  
25 owned by real people. Defendants knew that Apple would replace or  
26 repair the counterfeit Apple devices for genuine Apple devices or  
27 parts based on these false representations, and Apple did, in fact,

28



1 replace or repair these counterfeit Apple devices based on the  
2 fraudulent representations that defendants made to Apple.

3 e. Defendants SONG, JIANG, HU, LIN, and XING, and other  
4 co-conspirators, including runners that defendants hired for the  
5 scheme, fraudulently returned the counterfeit Apple devices to Apple  
6 in person at Apple stores or through the mail in the following ways:

7 i. Defendants SONG, JIANG, HU, LIN, and XING, and  
8 other co-conspirators, either visited Apple stores throughout the  
9 Central District of California for the service of the counterfeit  
10 Apple devices or processed service requests for the counterfeit Apple  
11 devices online. Defendants provided false reasons for the requested  
12 service of the counterfeit Apple devices, including that the devices  
13 would not power on, were physically damaged, or had other defects.  
14 Rather than provide their real residential addresses to Apple,  
15 defendants usually provided Apple with various mailboxes that they  
16 rented or caused to be rented for the scheme, along with aliases that  
17 they would occasionally use for the scheme. Defendants also  
18 deliberately misspelled their names, along with their mailing  
19 addresses, and added or removed extra characters to the mailing  
20 addresses to disguise the fact that the same persons processed  
21 numerous repairs and exchanges of Apple devices.

22 ii. Defendants SONG, JIANG, HU, LIN, and XING, and  
23 other co-conspirators, processed multiple service requests of  
24 counterfeit Apple devices on a given day, and sometimes visited  
25 multiple Apple stores throughout the Central District of California  
26 in a single day, where they fraudulently returned and attempted to  
27 return the counterfeit Apple devices for genuine Apple devices.

28

1           iii. During some of defendants' in-store visits, Apple  
2 sometimes replaced or repaired the counterfeit Apple device with a  
3 genuine Apple device in the same visit. On other occasions, Apple  
4 did not replace or repair the counterfeit Apple device during the  
5 same visit. In those cases, Apple either took the counterfeit Apple  
6 device from defendants during an in-store visit or directed  
7 defendants to mail the counterfeit Apple device directly to Apple  
8 repair centers. Apple then shipped, via a private and commercial  
9 interstate carrier, a genuine replacement Apple device or a repaired  
10 device to either the Apple store, where defendants returned to pick  
11 up the replacement Apple device, or to defendants at their various  
12 mailboxes throughout the Central District of California.

13           f. After they had successfully returned the counterfeit  
14 Apple devices for genuine Apple devices, defendants SONG, JIANG, HU,  
15 LIN, and XING, and other co-conspirators, shipped or caused to be  
16 shipped the genuine Apple devices to co-conspirators located in the  
17 United States and abroad, primarily in China, where the genuine Apple  
18 devices were resold at a substantial profit.

19           g. Through this fraudulent scheme, defendants SONG,  
20 JIANG, HU, LIN, and XING fraudulently returned and attempted to  
21 return over 16,000 counterfeit Apple devices, causing at least  
22 \$12.3 million in losses to Apple.

23       C.   OVERT ACTS

24           3. On or about the following dates, in furtherance of the  
25 conspiracy and to accomplish its objects, defendants SONG, JIANG, HU,  
26 LIN, and XING, and others known and unknown to the Grand Jury,  
27 committed and willfully caused others to commit the following overt  
28

1 acts, among others, in the Central District of California, and  
2 elsewhere:

3 Overt Act No. 1: On December 18, 2015, a co-conspirator sent  
4 defendant JIANG a list of counterfeit iPhones with valid Apple IMEI  
5 numbers corresponding to genuine, in-warranty iPhones.

6 Overt Act No. 2: On May 8, 2016, defendant JIANG sent  
7 defendant SONG electronic messages about changes in Apple's warranty  
8 repair program and discussed how the new policy would make it more  
9 difficult to fraudulently return counterfeit iPhones.

10 Overt Act No. 3: On May 20, 2016, defendant JIANG sent  
11 defendant SONG electronic messages indicating that an Apple employee  
12 at the Apple Irvine Spectrum store in Irvine, California, rejected a  
13 counterfeit iPad that he attempted to fraudulently return and told  
14 him it was not a genuine iPad.

15 Overt Act No. 4: On July 29, 2016, defendant JIANG sent an  
16 individual electronic messages about a potential job shipping and  
17 receiving counterfeit Apple devices.

18 Overt Act No. 5: On September 7, 2016, defendants SONG, LIN,  
19 and XING filled out applications for mail to be delivered to  
20 mailboxes at a UPS Store in Fountain Valley, California.

21 Overt Act No. 6: On September 21, 2016, defendants SONG and  
22 LIN submitted online repair requests for counterfeit iPhones that  
23 listed defendants SONG's and LIN's mailboxes at a UPS Store in  
24 Fountain Valley, California.

25 Overt Act No. 7: On December 7, 2016, defendants SONG, LIN,  
26 and XING filled out new applications for mail to be delivered to new  
27 mailboxes at a UPS Store in Fountain Valley, California.

1       Overt Act No. 8:     On December 16, 2016, defendant XING  
2 submitted an online repair request for a counterfeit iPhone and  
3 listed his mailing address as mailbox "#369&@" at a UPS Store in  
4 Montebello, California.

5       Overt Act No. 9:     On December 22, 2016, defendant XING  
6 submitted an online repair request for a counterfeit iPhone and  
7 listed his mailing address as mailbox "#221&@#" at a UPS Store in  
8 Fountain Valley, California.

9       Overt Act No. 10:    On December 23, 2016, defendant XING  
10 submitted an online repair request for a counterfeit iPhone and  
11 listed his mailing address as mailbox "#369@&#" at a UPS Store in  
12 Montebello, California.

13       Overt Act No. 11:   On December 24, 2016, defendant XING  
14 submitted an online repair request for a counterfeit iPhone and  
15 listed his mailing address as mailbox "#221@&#" at a UPS Store in  
16 Fountain Valley, California.

17       Overt Act No. 12:   On January 4, 2017, defendant JIANG filled  
18 out an application for mail to be delivered to a mailbox at a UPS  
19 Store in Walnut, California.

20       Overt Act No. 13:   On January 10, 2017, defendants SONG and  
21 XING rented mailboxes at a U.S. Post Office in Walnut, California.

22       Overt Act No. 14:   On February 8, 2017, defendant SONG  
23 instructed defendant JIANG, via electronic message, to use a new  
24 mailbox that was opened for Apple returns and to add a # symbol  
25 before and after the street number, remove letters from the street  
26 names, and add other random characters to disguise the addresses  
27 provided to Apple for the fraudulent returns of counterfeit Apple  
28 devices.

1        Overt Act No. 15:    On March 3, 2017, defendant XING submitted  
2 an online repair request for a counterfeit iPhone and listed his  
3 mailing address as mailbox "#221#" at a UPS Store in Fountain Valley,  
4 California.

5        Overt Act No. 16:    On April 1, 2017, defendant JIANG sent  
6 defendant SONG an electronic message containing a screenshot of a  
7 conversation that defendant JIANG had with an Apple customer service  
8 representative regarding a fraudulent return of a counterfeit Apple  
9 device.

10       Overt Act No. 17:    On April 1, 2017, defendant SONG responded  
11 to defendant JIANG's screenshot of a conversation with Apple customer  
12 service representative and told defendant JIANG to change the address  
13 used for the transaction.

14       Overt Act No. 18:    On April 6, 2017, defendant XING submitted  
15 an online repair request for a counterfeit iPhone and listed his  
16 mailing address as mailbox "#450#" at a UPS Store in Fountain Valley,  
17 California.

18       Overt Act No. 19:    On April 21, 2017, defendant SONG submitted  
19 an online repair request for a counterfeit iPhone and listed his  
20 mailing address with the incorrect spelling of the street address and  
21 the mailbox as mailbox "#119#" at a U.S. Post Office in Walnut,  
22 California.

23       Overt Act No. 20:    On July 3, 2017, defendants SONG and XING  
24 closed two rented mailboxes at a U.S. Post Office in Walnut,  
25 California.

26       Overt Act No. 21:    On May 1, 2018, defendant JIANG fraudulently  
27 returned a counterfeit iPhone at the Apple Los Cerritos store in  
28 Cerritos, California.

1        Overt Act No. 22:    On May 31, 2018, defendant SONG visited the  
2 Apple website from his residence in Corona, California, and made  
3 eight Apple Genius Bar appointments to fraudulently return  
4 counterfeit iPhones.

5        Overt Act No. 23:    On June 9, 2018, defendant LIN visited the  
6 Apple website from her residence in Corona, California, and made six  
7 Apple Genius Bar appointments to fraudulently return counterfeit  
8 iPhones.

9        Overt Act No. 24:    On July 14, 2018, defendant SONG  
10 fraudulently returned a counterfeit iPhone at the Apple Northridge  
11 store in Northridge, California.

12       Overt Act No. 25:    On July 14, 2018, defendant JIANG  
13 fraudulently returned and attempted to return three counterfeit  
14 iPhones at Apple stores within the Central District of California.

15       Overt Act No. 26:    On September 30, 2018, defendant JIANG sent  
16 an electronic message to an unknown co-conspirator indicating that he  
17 did not control when he received counterfeit Apple devices, stating  
18 that the bosses gave him the devices when they arrived.

19       Overt Act No. 27:    On October 3, 2018, defendant JIANG told an  
20 unknown co-conspirator to walk into an Apple store and attempt to  
21 repair, that is, fraudulently return, three counterfeit Apple devices  
22 for genuine Apple devices.

23       Overt Act No. 28:    On October 3, 2018, the unknown  
24 co-conspirator asked defendant JIANG if the unknown co-conspirator  
25 should use his own name for the return of the Apple devices.

26       Overt Act No. 29:    On October 3, 2018, defendant JIANG and an  
27 unknown co-conspirator complained to each other via electronic  
28 messages that Apple store employees were openly questioning their

1 multiple attempted returns of counterfeit Apple devices, with  
2 defendant JIANG complaining that Apple employees were very vigilant  
3 against them now.

4 Overt Act No. 30: On December 28, 2018, defendant HU  
5 fraudulently returned a counterfeit iPhone at the Apple Sherman Oaks  
6 store in Sherman Oaks, California.

7 Overt Act No. 31: On January 22, 2019, defendant SONG  
8 fraudulently returned a counterfeit iPhone at the Apple Los Cerritos  
9 store in Cerritos, California.

10 Overt Act No. 32: On January 26, 2019, defendants LIN and XING  
11 fraudulently returned four counterfeit iPhones at the Apple Victoria  
12 Gardens store in Rancho Cucamonga, California.

13 Overt Act No. 33: On February 28, 2019, defendant HU sent an  
14 electronic message to an individual indicating that she received \$5  
15 for every counterfeit Apple device that other co-conspirators  
16 fraudulently returned to Apple stores.

17 Overt Act No. 34: On March 5, 2019, defendant LIN fraudulently  
18 returned a counterfeit iPhone at the Apple Los Cerritos store in  
19 Cerritos, California.

20 Overt Act No. 35: On March 8, 2019, defendants LIN and XING  
21 fraudulently returned a counterfeit iPhone at the Apple South Coast  
22 Plaza store in Costa Mesa, California.

23 Overt Act No. 36: On March 21, 2019, defendants LIN and XING  
24 fraudulently returned a counterfeit iPhone at the Apple Fashion  
25 Island store in Newport Beach, California.

26 Overt Act No. 37: On January 10, 2020, defendant LIN visited  
27 the Apple website from her residence in Corona, California, and made  
28

1 three Apple Genius Bar appointments to fraudulently return  
2 counterfeit iPhones.

3 Overt Act No. 38: On January 21, 2020, defendant XING visited  
4 three different Apple Stores in Costa Mesa, Newport Beach, and  
5 Cerritos, California, where he fraudulently returned counterfeit  
6 iPhones.

7 Overt Act No. 39: On May 12, 2021, defendants JIANG and HU  
8 discussed returning counterfeit Apple watches.

9 Overt Act No. 40: On August 29, 2021, defendant HU filled out  
10 an application for mail to be delivered to mailbox "249" at a private  
11 business in San Gabriel, California.

12 Overt Act No. 41: On December 16, 2021, defendant SONG visited  
13 five different Apple stores in Brea, Cerritos, Manhattan Beach, Los  
14 Angeles, and Beverly Hills, California, where he fraudulently  
15 returned and attempted to return a total of six counterfeit Apple  
16 devices.

17 Overt Act No. 42: On June 9, 2022, defendant SONG visited six  
18 different Apple stores in Los Angeles, Beverly Hills, Manhattan  
19 Beach, Pasadena, and Glendale, California, where he fraudulently  
20 returned and attempted to return a total of ten counterfeit Apple  
21 devices.

22 Overt Act No. 43: On September 23, 2022, defendant SONG  
23 visited six different Apple stores in Pasadena, Glendale, Los  
24 Angeles, Beverly Hills, Cerritos, Costa Mesa, and Irvine, where he  
25 fraudulently returned and attempted to return counterfeit Apple  
26 devices.



1        Overt Act No. 44:    On November 16, 2022, defendant JIANG  
2 fraudulently returned two counterfeit iPads at the Apple Century City  
3 store in Los Angeles, California.

4        Overt Act No. 45:    On November 16, 2022, defendant SONG  
5 fraudulently returned a counterfeit iPhone at the Apple Brea Mall  
6 store in Brea, California.

7        Overt Act No. 46:    On November 16, 2022, defendant HU  
8 fraudulently returned a counterfeit iPad at the Apple The Americana  
9 at Brand store in Glendale, California.

10       Overt Act No. 47:    On December 2, 2022, defendant JIANG sent an  
11 electronic message to defendant HU that a person described in  
12 Mandarin Chinese as the "second boss" instructed them to stop  
13 visiting the Apple The Grove store in Los Angeles, California,  
14 because the store changed its policy and only permitted one  
15 appointment per person per day, and because certain Apple store  
16 employees were openly questioning defendants' repeated visits to the  
17 Apple store.

18       Overt Act No. 48:    On December 7, 2022, defendant SONG  
19 fraudulently returned a counterfeit iPhone at the Apple Pasadena  
20 store in Pasadena, California.

21       Overt Act No. 49:    On December 8, 2022, defendants JIANG and HU  
22 agreed to not visit a particular Apple store after an Apple employee  
23 rejected defendant HU's attempted return of a counterfeit iPad, with  
24 defendant HU telling defendant JIANG that the employee told defendant  
25 HU that the Apple logo on the back of her iPad reflected light  
26 differently than other iPads.

27       Overt Act No. 50:    On December 8, 2022, defendant HU  
28 fraudulently returned a counterfeit iPad, filled with metal weights

1 inside to mimic the weight of a genuine iPad, at the Apple The  
2 Americana at Brand store in Glendale, California

3 Overt Act No. 51: On December 8, 2022, defendant SONG  
4 instructed defendant HU to attempt to fraudulently return previously  
5 rejected counterfeit Apple devices at Best Buy rather than Apple  
6 stores because Best Buy would not track returns of counterfeit Apple  
7 devices previously attempted at Apple stores.

8 Overt Act No. 52: On December 8, 2022, defendant HU sent an  
9 electronic message to defendant JIANG about the second boss directing  
10 her to fraudulently return counterfeit Apple devices at Best Buy.

11 Overt Act No. 53: On December 9, 2022, defendant JIANG  
12 fraudulently returned a counterfeit iPad, filled with metal weights  
13 inside to mimic the weight of a genuine iPad, at the Apple Manhattan  
14 Village store in Manhattan Beach, California.

15 Overt Act No. 54: On December 9, 2022, defendant SONG  
16 fraudulently returned a counterfeit iPad, filled with metal weights  
17 inside to mimic the weight of a genuine iPad, at the Apple Brea Mall  
18 store in Brea, California.

19 Overt Act No. 55: On December 12, 2022, defendants HU and  
20 JIANG discussed an Apple store employee rejecting their recent  
21 attempts to fraudulently return counterfeit Apple devices and how  
22 their boss would be angry.

23 Overt Act No. 56: On December 12, 2022, defendant HU  
24 fraudulently returned a counterfeit iPad at the Apple Brea Mall store  
25 in Brea, California.

26 Overt Act No. 57: On January 7, 2023, defendants HU and JIANG  
27 discussed a person described in Mandarin Chinese as their "big boss"  
28 via electronic messages and defendant JIANG said that he had never

1 been in contact with him, but that the boss was from Huaqiangbei,  
2 China, and had many family businesses.

3 Overt Act No. 58: On January 8, 2023, defendant HU sent an  
4 electronic message to defendant JIANG that she was able to  
5 fraudulently return a counterfeit iPad at the Apple Beverly Center  
6 store in Los Angeles, California, despite it looking fake to her.

7 Overt Act No. 59: On January 8, 2023, defendant JIANG  
8 fraudulently returned and attempted to return ten counterfeit Apple  
9 devices to multiple Apple stores within the Central District of  
10 California.

11 Overt Act No. 60: On January 9, 2023, defendants JIANG and HU  
12 discussed with each other via electronic messages how Apple store  
13 employees were annoyed with them after an Apple store manager asked a  
14 lot of questions about their repeated returns at the Apple store.

15 Overt Act No. 61: On January 10, 2023, defendant HU sent an  
16 electronic message to defendant SONG indicating that the Apple  
17 Manhattan Village store in Manhattan Beach, California, rejected her  
18 fraudulent return of a counterfeit Apple device.

19 Overt Act No. 62: On January 11, 2023, defendants HU and JIANG  
20 exchanged electronic messages about seeing other unknown co-  
21 conspirators, who worked for their big boss, making returns at Apple  
22 stores.

23 Overt Act No. 63: On May 10, 2023, defendant SONG attempted to  
24 fraudulently return a counterfeit Apple device, that an Apple  
25 employee had previously rejected several days earlier, at the Apple  
26 Victoria Gardens store in Rancho Cucamonga, California.

27 Overt Act No. 64: On October 7, 2023, defendant SONG attempted  
28 to fraudulently return a counterfeit Apple device, that defendant

1 JIANG had previously attempted to return, at the Apple Fashion Island  
2 store in Newport Beach, California.

3 Overt Act No. 65: On October 26, 2023, defendant JIANG visited  
4 eight different Apple stores within the Central District of  
5 California, where he fraudulently returned and attempted to return  
6 counterfeit iPads.

7 Overt Act No. 66: On October 27, 2023, defendant SONG visited  
8 six different Apple stores within the Central District of California,  
9 where he fraudulently returned and attempted to return counterfeit  
10 iPads.

11 Overt Act No. 67: On November 25, 2023, defendant SONG visited  
12 ten different Apple stores within the Central District of California,  
13 where he fraudulently returned and attempted to return fourteen  
14 counterfeit Apple devices.

15 Overt Act No. 68: On December 27, 2023, defendant JIANG  
16 fraudulently returned and attempted to return five counterfeit Apple  
17 devices online and at Apple stores within the Central District of  
18 California.

19 Overt Act No. 69: On February 8, 2024, defendant SONG visited  
20 Apple stores in Los Angeles, Newport Beach, Brea, and Rancho  
21 Cucamonga, California, where he fraudulently returned and attempted  
22 to return five counterfeit Apple devices.

23 Overt Act No. 70: On March 12, 2024, defendant SONG visited  
24 the Apple Victoria Gardens store in Rancho Cucamonga, California,  
25 where he fraudulently attempted to return a counterfeit Apple device.

COUNT TWO

[18 U.S.C. §§ 1028A(a)(1), 2(a)]

[ALL DEFENDANTS]

Beginning on an unknown date but no later than December 18, 2015, and continuing through at least March 12, 2024, in Los Angeles, San Bernardino, Riverside, and Orange Counties, within the Central District of California, and elsewhere, defendants YANG SONG, JUNWEI JIANG, ZHENGXUAN HU, YUSHAN LIN, and SHUYI XING, each aiding and abetting each other, knowingly transferred, possessed, and used, without lawful authority, and willfully caused another person to knowingly transfer, possess, and use, without lawful authority, means of identification that defendants knew belonged to other persons, namely, international mobile equipment identity numbers of real Apple iPhone and iPad owners, during and in relation to the offense of conspiracy to commit wire fraud and mail fraud, a felony violation of Title 18, United States Code, Section 1349, as charged in Count One of this Indictment.

1 COUNTS THREE THROUGH NINE

2 [18 U.S.C. § 1343]

3 [ALL DEFENDANTS]

4 The Grand Jury hereby realleges and incorporates by reference  
5 paragraphs 1 through 7 of the Introductory Allegations and  
6 Definitions of this Indictment as though fully set forth herein.

7 A. THE SCHEME TO DEFRAUD

8 1. Beginning on an unknown date but no later than December 18,  
9 2015, and continuing through at least March 12, 2024, in Los Angeles,  
10 San Bernardino, Riverside, and Orange Counties, within the Central  
11 District of California, and elsewhere, defendants YANG SONG ("SONG"),  
12 JUNWEI JIANG ("JIANG"), ZHENGXUAN HU ("HU"), YUSHAN LIN ("LIN"), and  
13 SHUYI XING ("XING"), and other persons known and unknown to the Grand  
14 Jury, knowingly and with intent to defraud, devised, participated in,  
15 and executed a scheme to defraud Apple as to material matters, and to  
16 obtain money and property by means of material false and fraudulent  
17 pretenses, representations, and promises, and the concealment of  
18 material facts.

19 2. The scheme operated, in substance, as set forth in  
20 paragraph 2 of Count One of this Indictment, which is realleged and  
21 incorporated herein by reference as if set forth in full.

22 B. USE OF INTERSTATE WIRES

23 3. On or about the following dates, in the Central District of  
24 California, and elsewhere, defendants SONG, JIANG, HU, LIN, and XING,  
25 for the purpose of executing the above-described scheme to defraud,  
26 transmitted and willfully caused the transmission of the following  
27 items by means of wire and radio communication in interstate  
28 commerce:

COUNT	DATE	INTERSTATE WIRE TRANSMISSION
THREE	11/20/2019	Email from Apple to defendant XING's Yahoo email account, relating to defendant XING's drop-off of an iPhone (Apple Repair ID R436984491), at the Apple Los Cerritos store in Cerritos, California
FOUR	12/3/2019	Email from Apple to defendant SONG's Yahoo email account, relating to defendant SONG's drop-off of an iPhone (Apple Repair ID R438396805), at the Apple South Coast Plaza store in Costa Mesa, California
FIVE	7/22/2021	Email from Apple to defendant SONG's Yahoo email account, relating to defendant SONG's drop-off of an iPad (Apple Repair ID R501125497), at the Apple Manhattan Village store in Manhattan Beach, California
SIX	9/23/2022	Email from Apple to defendant SONG's Yahoo email account, relating to defendant SONG's drop-off of an iPod (Apple Repair ID R553161165), at the Apple Irvine Spectrum store in Irvine, California
SEVEN	11/17/2022	Email from Apple to defendant HU's Google email account, relating to defendant HU's drop-off of an iPad (Apple Repair ID R560915547), at the Apple The Grove store in Los Angeles, California
EIGHT	12/8/2022	Email from Apple to defendant HU's Google email account, relating to defendant HU's drop-off of an iPad (Apple Repair ID R563369917), at the Apple The Americana at Brand store in Glendale, California
NINE	1/11/2023	Email from defendant HU's Google email account to defendant JIANG's Microsoft email account, relating to defendant HU's drop-off of an iPad (Apple Repair ID R566490299), at the Apple Fashion Island store in Newport Beach, California

1                                    COUNTS TEN THROUGH TWENTY-ONE

2                                    [18 U.S.C. § 1341]

3                                    [ALL DEFENDANTS]

4            The Grand Jury hereby realleges and incorporates by reference  
5 paragraphs 1 through 7 of the Introductory Allegations and  
6 Definitions of this Indictment as though fully set forth herein.

7    A.    THE SCHEME TO DEFRAUD

8            1.    Beginning on an unknown date but no later than December 18,  
9 2015, and continuing through at least March 12, 2024, in Los Angeles,  
10 San Bernardino, Riverside, and Orange Counties, within the Central  
11 District of California, and elsewhere, defendants YANG SONG ("SONG"),  
12 JUNWEI JIANG ("JIANG"), ZHENGXUAN HU ("HU"), YUSHAN LIN ("LIN"), and  
13 SHUYI XING ("XING"), and other persons known and unknown to the Grand  
14 Jury knowingly and with intent to defraud, devised, participated in,  
15 and executed a scheme to defraud Apple as to material matters, and to  
16 obtain money and property by means of material false and fraudulent  
17 pretenses, representations, and promises, and the concealment of  
18 material facts.

19            2.    The scheme operated, in substance, as set forth in  
20 paragraph 2 of Count One of this Indictment, which is realleged and  
21 incorporated herein by reference as if set forth in full.

22    B.    USE OF THE MAILS

23            3.    On or about the following dates, in Los Angeles, San  
24 Bernardino, Riverside, and Orange Counties, within the Central  
25 District of California, and elsewhere, defendants SONG, JIANG, HU,  
26 LIN, and XING, for the purpose of executing the above-described  
27 scheme to defraud, deposited and caused to be deposited and to be  
28 sent and delivered by a private and commercial interstate carrier,



1 and knowingly caused to be delivered by such carrier according to the  
 2 directions thereon, the following items:

COUNT	DATE	ITEM MAILED
TEN	6/4/2019	A FedEx package, bearing FedEx Tracking Number 101911346001, containing a genuine replacement iPhone (Apple Repair ID R419283235), that was shipped from Apple to defendant XING at a UPS Store in Corona, California
ELEVEN	6/5/2019	A FedEx package, bearing FedEx Tracking Number 101911376633, containing a genuine replacement iPhone (Apple Repair ID R419282523), that was shipped from Apple to defendant LIN at a UPS Store in Corona, California
TWELVE	8/29/2019	A FedEx package, bearing FedEx Tracking Number 119431684055, containing a genuine replacement iPhone (Apple Repair ID R433951570), that was shipped from Apple to defendant XING at a UPS Store in Corona, California
THIRTEEN	9/20/2021	A FedEx package, bearing FedEx Tracking Number 531855622285, containing a genuine replacement iPad (Apple Repair ID R507863167), that was shipped from Apple to defendant JIANG at a UPS Store in San Gabriel, California
FOURTEEN	11/16/2022	A FedEx package, bearing FedEx Tracking Number 615184082266, containing a genuine replacement iPad (Apple Repair ID R560811657), that was shipped from Apple to defendant HU at defendant HU's residence in Alhambra, California
FIFTEEN	12/7/2022	A FedEx package, bearing FedEx Tracking Number 615184257205, containing a genuine replacement iPad (Apple Repair ID R563127201), that was shipped from Apple to defendant HU at defendant HU's residence in Alhambra, California
SIXTEEN	12/9/2022	A FedEx package, bearing FedEx Tracking Number 614658610388, containing a genuine replacement iPad (Apple Repair ID R563496767), that was shipped from Apple to defendant JIANG at a UPS store in San Gabriel, California

COUNT	DATE	ITEM MAILED
SEVENTEEN	12/29/2022	A FedEx package, bearing FedEx Tracking Number 621290822049, containing a genuine replacement iPad (Apple Repair ID R565427913), that was shipped from Apple to defendant SONG at a UPS store in Corona, California
EIGHTEEN	12/31/2022	A FedEx package, bearing FedEx Tracking Number 621290854011, containing a genuine replacement iPad (Apple Repair ID R565554515), that was shipped from Apple to defendant JIANG at a UPS store in San Gabriel, California
NINETEEN	1/11/2023	A FedEx package, bearing FedEx Tracking Number 619490072460, containing a genuine replacement iPad (Apple Repair ID R564735063), that was shipped from Apple to defendant HU at a UPS Store in San Gabriel, California
TWENTY	1/12/2023	A FedEx package, bearing FedEx Tracking Number 628056578882, containing a genuine replacement iPad (Apple Repair ID R566798037), that was shipped from Apple to defendant SONG at a UPS Store in Corona, California
TWENTY-ONE	9/6/2023	A FedEx package, bearing FedEx Tracking Number 704643881775, containing a genuine replacement iPad (Apple Repair ID R595039663), that was shipped from Apple to defendant SONG at defendant SONG's residence in Corona, California

COUNT TWENTY-TWO

[18 U.S.C. § 2320(a)(1)]

[ALL DEFENDANTS]

The Grand Jury hereby realleges and incorporates by reference paragraphs 1 through 7 of the Introductory Allegations and Definitions of this Indictment as though fully set forth herein.

A. OBJECT OF THE CONSPIRACY

1. Beginning on an unknown date but no later than December 18, 2015, and continuing through at least March 12, 2024, in Los Angeles, San Bernardino, Riverside, and Orange Counties, within the Central District of California, and elsewhere, defendants YANG SONG, JUNWEI JIANG, ZHENGXUAN HU, YUSHAN LIN, and SHUYI XING intentionally conspired and agreed with one another, and with other persons known and unknown to the Grand Jury, to intentionally traffic in goods and knowingly use a counterfeit mark on or in connection with such goods, in violation of Title 18, United States Code, Section 2320(a)(1).

B. MANNER AND MEANS OF THE CONSPIRACY

2. The object of the conspiracy was to be accomplished, in substance, as follows:

a. The Grand Jury realleges paragraphs 2.a through 2.g of Count One of this Indictment as though fully set forth herein.

C. OVERT ACTS

3. On or about the following dates, in furtherance of the conspiracy and to accomplish its object, defendants SONG, JIANG, HU, LIN, and XING, and others known and unknown to the Grand Jury, committed and willfully caused others to commit the following overt acts, among others, in the Central District of California, and elsewhere:

1        Overt Act Nos. 1-70: The Grand Jury realleges and incorporates  
2 Overt Act Number 1 through Overt Act Number 70 of Section C of Count  
3 One of this Indictment as though fully set forth herein.

FORFEITURE ALLEGATION ONE

[18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c)]

1. Pursuant to Rule 32.2 of the Federal Rules of Criminal Procedure, notice is hereby given that the United States of America will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), in the event of any defendant's conviction of any of the offenses set forth in Counts One through Twenty-One of this Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

(a) All right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds traceable to the offenses; and

(b) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraph (a).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c), any defendant so convicted shall forfeit substitute property, up to the value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph or any portion thereof

(a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to, or deposited with a third party;

(c) has been placed beyond the jurisdiction of the court; (d) has been substantially diminished in value; or (e) has been commingled with other property that cannot be divided without difficulty.

FORFEITURE ALLEGATION TWO

[18 U.S.C. § 2323(b) and 28 U.S.C. § 2461(c)]

1 Pursuant to Rule 32.2 of the Federal Rules of Criminal  
2 Procedure, notice is hereby given that the United States of America  
3 will seek forfeiture as part of any sentence, pursuant to Title 18,  
4 United States Code, Section 2323(b) and Title 28, United States Code,  
5 Section 2461(c), in the event of any defendant's conviction of the  
6 offense set forth in Count Twenty-Two of this Indictment.  
7

8 2. Any defendant so convicted shall forfeit to the United  
9 States of America the following:  
10

11 (a) All right, title, and interest in any article made or  
12 trafficked in violation of 18 U.S.C. § 2320;

13 (b) All right, title, and interest in any property used,  
14 or intended to be used, in any manner or part to commit or facilitate  
15 the commission of an offense referred to in subparagraph (a);

16 (c) All right, title, and interest in any property  
17 constituting or derived from any proceeds obtained directly or  
18 indirectly as a result of the commission of an offense referred to in  
19 subparagraph (a); and

20 (d) To the extent such property is not available for  
21 forfeiture, a sum of money equal to the total value of the property  
22 described in subparagraphs (a), (b), and (c).

23 3. Pursuant to Title 21, United States Code, Section 853(p),  
24 as incorporated by Title 18, United States Code, Section 2323(b) (2)  
25 and Title 28, United States Code, Section 2461(c), any defendant so  
26 convicted shall forfeit substitute property, up to the value of the  
27 property described in the preceding paragraph if, as the result of  
28 any act or omission of said defendant, the property described in the

1 preceding paragraph or any portion thereof (a) cannot be located upon  
2 the exercise of due diligence; (b) has been transferred, sold to, or  
3 deposited with a third party; (c) has been placed beyond the  
4 jurisdiction of the court; (d) has been substantially diminished in  
5 value; or (e) has been commingled with other property that cannot be  
6 divided without difficulty.

7  
8 A TRUE BILL

9  
10 /s/  
11 Foreperson

12 E. MARTIN ESTRADA  
13 United States Attorney

14 

15 CAMERON L. SCHROEDER  
16 Assistant United States Attorney  
17 Chief, National Security Division

18 KHALDOUN SHOBAKI  
19 Assistant United States Attorney  
20 Chief, Cyber & Intellectual  
21 Property Crimes Section

22 LAUREN E. RESTREPO  
23 Deputy Chief, Cyber &  
24 Intellectual Property Crimes  
25 Section

26 ANDREW M. ROACH  
27 Assistant United States Attorney  
28 Cyber & Intellectual Property  
Crimes Section